

REMARKS/ARGUMENTS

The Applicant acknowledges, with thanks, the office action dated October 17, 2008. Examiner's withdrawal of the finality of the previous office action is noted with appreciation. Claims 1-16, 26, and 28 are currently pending.

Non-Art Matters

Claims 1 and 9 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Accordingly, claims 1 and 9 have been amended to address the Examiner's rejection. The limitation concerning authenticating using a second authentication protocol responsive to the authorization failure has been deleted. The limitation concerning signaling an authorization failure to the peer and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials is supported by the specification (see ¶33; "On concluding the distribution of the credential or set of credentials, ADHP concludes with an authorization failure, to signal that while credentials have been provisioned, network access is denied until the parties ensue in an actual authentication (versus) provisioning protocol."). Therefore, withdrawal of the rejection is respectfully requested.

Prior-Art Matters

Claims 1-16, 26, and 28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-tls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40 (*hereinafter*, "Funk") in view of U.S. Patent Application Publication No. 2005/0071677 to Khanna (*hereinafter*, "Khanna").

Independent claim 1, as currently amended, recites a method for secure communication. A secure tunnel is established between a server and a peer using an encryption algorithm that establishes an encryption key. The peer is then authenticated with the server over the secured tunnel establishing an authentication key. The server verifies that the peer possesses the same encryption and authentication keys as the server. In response, a network access credential is then

provisioned to the peer using the secured tunnel. Upon conclusion of the provisioning of the network access credential and prior to the peer authenticating using the provisioned credentials, an authorization failure is signaled to the peer. The peer is denied access to the network by the server until the peer authenticates using the provisioned credentials. Independent claim 9 recites an implementation for of independent claim 1. No new matter has been added as the amendments are supported by the original specification (see ¶33).

By contrast, Funk uses EAP-TTLS to gain access to the network. Once a successful authentication has occurred, keys are distributed and a session is initiated between the client and the network. Funk does not teach signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisioned credentials, and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials. The Office Action relies on sections 4.3, 6-6.2, and 10 of Funk to teach signaling an authorization failure to the peer and denying access to the peer until the peer authenticates using the provisioned credentials. Applicant respectfully disagrees with the Office Action's reliance on Funk.

Sections 4.3, 6-6.2, and 10 of Funk discusses messaging. Specifically, two phase negotiation is discussed. During the first phase, a server is authenticated to a client based on a public/private key certificate. This creates a TLS record layer channel to secure subsequent communications. During the second phase, the client and the server use the established TLS record layer as a tunnel to exchange further information such as client authentication. The client begins the phase two exchange by sending authentication information to the server. The server responds by either sending key distribution information to the client or sending the authentication information received to an authentication server. This process continues until the server has enough information to issue either a success or a failure to the client. Thus, the server does not signal an authorization failure to the peer upon conclusion of the provisioning of the network access credentials, prior to the peer authenticating using the provisioned credentials, nor does the server deny the peer access to the network until the peer authenticates using the provisioned credentials as taught by claims 1 and 9. Rather, Funk teaches signaling an authorization failure to the client after the client sends authentication information to the server.

The aforementioned deficiencies in Funk are not remedied by any teaching of Khanna. Khanna teaches a method for authenticating clients and boot server hosts to provide a secure

network boot environment. Messages are exchanged between a client and a boot server or authentication server proxy for the boot server during pre-boot operations of the client to authentic the boot server and the client. Kahanna states that authentication credentials can be provisioned to the device (§ 19). However, Khanna does not teach or suggest signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisioned credentials, and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials. Moreover, Khanna does not teach or suggest setting up a secure tunnel and authenticating within the tunnel before receiving the provisioned credential. Khanna only mentions using public/private keys and/or EAP to instatiate a shared key (§ 20). Moreover, Khanna is relied on the Office Action to teach a second authenticating protocol by the peer responsive to an authorization failure, which does not remedy the aforementioned deficiencies in Funk. Thus, neither Funk nor Khanna, alone or in combination, teach or suggest each and every element of independent claims 1 and 9. Therefore, for the reasons set forth, withdrawal of this rejection is respectfully requested.

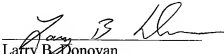
Claims 2-8 and 28 depend directly from claim 1 and therefore contain each and every element of claim 1. Claims 10-16 and 26 depend directly from claim 9 and therefore contain each and every element of claim 9. Therefore, for the same reasons set forth for claims 1 and 9, withdrawal of rejections of 2-8, 10-16, 26, and 28 is respectfully requested.

Conclusion

Withdrawal of the rejections to this application is requested for the reasons set forth herein and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: 1-14-09


Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009